Quick Start Guide
Fidelis Network®
Direct/Internal
Sensor in AWS

Fidelis Cybersecurity
4500 East-West Highway, Suite 400
Bethesda, MD 20814

Fidelis Network®

Fidelis Network Direct/Internal Sensor in AWS, Revised 2019

While we have done our best to ensure that the material found in this document is accurate, **Fidelis Cybersecurity** makes no guarantee that the information contained herein is error free.

Fidelis Network includes GeoLite data created by MaxMind, available from http://www.maxmind.com/

Table of Contents

Sensor Overview 1
Documentation and References 1
Fidelis Network Sensor on AWS Access 1
Technical Support 1
Sensor NetworkingEnvironment....... 2
Management (Admin) Network....... 2
Monitored Networks 2
Deployment and Configuration 3
Configure the Sensor....... 4
Register the Sensor with CommandPost....... 4
Upgrading the Sensor....... 5

Sensor Overview

Fidelis Network sensors are the components that monitor the network environment for activities that may indicate advanced threat, malware, and data theft. These sensors analyze network traffic, deliver alerts and session data to CommandPost, and deliver non-selective network session metadata to Fidelis Collector for retrospective analysis.

The Fidelis Network sensor on AWS **requires** an existing Fidelis Network installation with CommandPost and a Collector to which the sensor can connect..

Fidelis sensors report network alerts and network metadata to your on-premises Fidelis Network components or to the remote Fidelis Network Cloud components hosted by Fidelis or in your private cloud. Your configuration will depend on which environment you are working with.

Documentation and References

Fidelis Network product documentation, appliance specifications, and instructions can be found at: https://www.fidelissecurity.com or through the ⓘ icon at the CommandPost GUI.

Fidelis Network Sensor on AWS Access

Command line access to the sensor is available through SSH using the certificate generated or selected at launch time with the username: `fidelis`.

Technical Support

For all technical support related to this product, check with your site administrator to determine support contract details. For support of your product, contact your reseller. If you have a direct support contract with Fidelis Cybersecurity, contact the Fidelis Cybersecurity support team at:

Phone: +1 301.652.7190

Toll-free in the US: 1.800.652.4020 – Use the customer support option.

Email: support@fidelissecurity.com

Web: https://support.fidelissecurity.com

Sensor Networking Environment

Sensor appliances will connect to . at least two VPCs/subnets for service and monitoring. Use the tables below to identify how many and what type of network interfaces you will need for your deployment.

Management (Admin) Network

The Admin Network connects Fidelis Network sensors to the CommandPost, Collector, and Fidelis Insight Cloud. The Admin Network interface should be associated with a VPC subnet that can route to an Internet Gateway. All data between the sensor and the CommandPost will be encapsulated in an encrypted channel (TLS) or a point-to-point VPN tunnel depending on your configuration).

Monitored Networks

These interfaces connect the sensor appliance to the monitored networks through a traffic mirroring service. The sensor is capable of receiving ERSPAN or VXLAN encapsulated traffic in any subnet or VPC that is routable to the traffic mirroring service running in the cloud. In the AWS cloud, the Fidelis Direct/Internal sensors inter-operate with and can receive traffic from following traffic mirror services:

AWS VPC Traffic Mirror that uses VXLAN

Netgate TNSR that uses ERSPAN

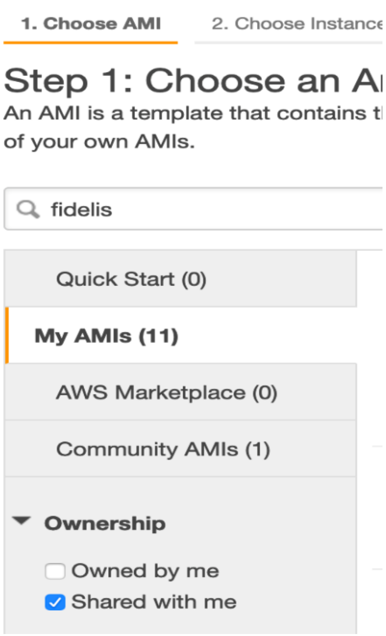
Deployment and Configuration

Each network interface must be associated with a logical network. Build a table of the logical information for each appliance (example below) that you can reference during configuration.

The primary interface (eth0) is associated with a management network that has access to the CommandPost via IP routing.

The secondary interfaces are associated with networks to be monitored. These networks are VPC subnets.

Basic instructions for deploying the sensor:



1. Choose AMI

2. Choose Instance

Step 1: Choose an A

An AMI is a template that contains t of your own AMIs.

fidelis

Quick Start (0)

My AMIs (11)

AWS Marketplace (0)

Community AMIs (1)

Ownership

□ Owned by me

☑ Shared with me

1. Fidelis will privately share the AMI of the sensor with your AWS subscription id.
2. Log into the AWS console.
3. Navigate to https://console.aws.amazon.com/ec2/
4. Click Instances.
5. Click Launch Instance to enter the Launch Instance Wizard.
6. Click “My AMIs”, then filter for “Shared with me” under the Ownership section. If needed, search for fidelis in the top search bar.
7. Find the entry for Fidelis Network Sensor then click Select.
8. Click Continue on the information page.
9. Choose Instance Type. The recommended instance type depends on the CPU and RAM resources of the sensor. Click Next.
   Refer to chapter 3 Virtual Appliances of the *Enterprise Setup and Configuration Guide* for details.
10. Configure Instance Details:
    a. Select the VPC and management subnet in which to launch the instance.

    b. Add storage if this instance will require more than the default 40GB disk, then click Next.

    c. Add Tags to identify this instance. It’s advisable to set the Name tag to a user-friendly identifier and Click Next.

    d. Configure a Security Group to allow SSH (TCP 22) access to the sensor.
    Note: Fidelis recommends that the allowed Source be limited to a specific address or network that will be used to connect to the Fidelis Network sensor instance.

    e. Give the security group a name such as: Fidelis Network Sensor management”
11. Verify the settings selected in earlier steps, then click Launch.
12. Select an SSH key or create a new key in the popup. Click Launch Instances.
13. In the instances pane, select the instance and copy the public IP address.

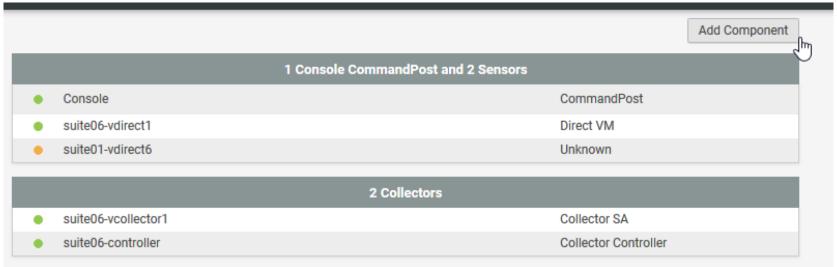
Configure the Sensor

This Quick Start Guide will help you configure a Sensor in "tap" or "out-of-band" mode, where each monitoring interface is connected to a different network. The Cloud traffic visibility works in out-of-band mode, with each monitored network interface needing IP network configuration for that interface. Sensors will need to be configured to support ERSPAN or VXLAN depending on the encapsulation technology used by the traffic source. For help with these configurations, refer to the Fidelis Network *Enterprise Setup and Configuration Guide*.

Register the Sensor with CommandPost

Note: If registering the sensor to an on-premise CommandPost, additional networking and firewall changes may be needed.

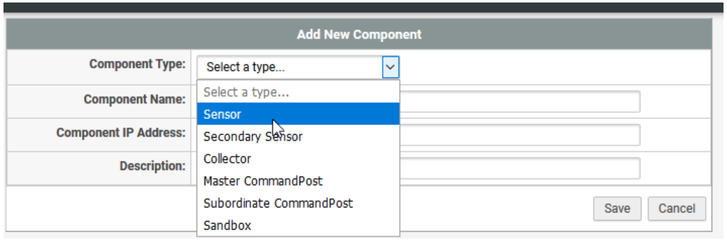
1. Log into the CommandPost GUI from a web browser.
2. Navigate to the Administration / System / Components page.



	1 Console CommandPost and 2 Sensors	
●	Console	CommandPost
●	suite06-vdirect1	Direct VM
●	suite01-vdirect6	Unknown

	2 Collectors	
●	suite06-vcollector1	Collector SA
●	suite06-controller	Collector Controller

3. Click Add Component and select Sensor. Complete the form:



Add New Component

Component Type: Select a type...

Component Name:

Component IP Address:

Description:

Component Type – Select Sensor

Component Name — this is a user-friendly name for the Sensor, not the FQDN of the Sensor

Component IP address — the IP address of the ADMIN interface of the Sensor appliance

Description — an optional label for the component such as: location or business unit.

4. Click Save.
   The sensor's component name will appear on the on the Components page. Click the component name to view Details.
5. Click Register and accept the End User License Agreement (EULA). The Command Post will then communicate with the sensor at the specified IP address.

Upgrading the Sensor

Once the sensor is registered with the CommandPost, it may need to be upgraded to match the rest of the system. A sensor that is running an older version may not function correctly.

Navigate to the Administration / System / Version Control page. If the sensor Installed version does not match the CommandPost, click the box next to the sensor name and select Install.